UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/725,881	12/02/2003	Anthony J. Yeates	M61.12-0564	3385

27366 7590 10/03/2007

WESTMAN CHAMPLIN (MICROSOFT CORPORATION)
SUITE 1400
900 SECOND AVENUE SOUTH
MINNEAPOLIS, MN 55402-3319

EXAMINER	
DADA, BEEMNET W	

ART UNIT	PAPER NUMBER
2135	

MAIL DATE	DELIVERY MODE
10/03/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/725,881	YEATES ET AL.	
	Examiner	Art Unit	
	Beemnet W. Dada	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 December 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-29* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-29* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *3/17/04*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-29 have been examined.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. Claims 1-29 are rejected under 35 U.S.C. 102(b) as being anticipated by Jancula US 2002/0023208 A1.

4. As per claim 1, Jancula teaches a computer-implemented method for enhancing the security of communication over a network, the method comprising:

receiving a set of authentication credentials from a user [paragraphs 0056-0057 and 0069-0071];

receiving from the user a request that requires communication over the network with a remote system [paragraphs 0056-0057 and 0070-0073];

applying a collection of security privileges to the set of authentication credentials to determine if the user is authorized to carry out the request [paragraphs 0057-0058 and 0071-0075];

selectively transmitting a security certificate over the network to the remote system, the certificate containing a public key [paragraphs 0056-0057];

receiving from the remote system a session ticket that has been encrypted with the public key [paragraph 0088];

decrypting the session ticket with a corresponding private key [paragraph 0089-0091];

using the session ticket as an authenticator for subsequent communications with the remote system [paragraphs 0093-0096].

5. As per claim 12, Jancula teaches a computer-implemented method for enhancing the security of communication over a network, the method comprising:

generating a public key and a corresponding private key [paragraph 0056];

storing the private key [paragraph 0056];

transmitting the public key over the network to a registration service [paragraphs 0056-0057];

receiving from the registration service a security certificate that includes the public key [paragraphs 0056-0057];

transmitting the security certificate over the network to an entity with which a channel of communication is desired [paragraphs 0056-0057];

receiving from the entity a session ticket encrypted with the public key [paragraphs 0060 and 0088];

decrypting the session ticket with the private key [paragraphs 0061 and 0089-0091]; and

using the session ticket as an authenticator for subsequent communications with the entity [paragraphs 0062 and 0093-0096].

6. As per claim 18, Jancula teaches a communication security system for facilitating the enhancement of the security of communications over a network, the system comprising:

a client application configured to respond to a user request for service by retrieving a security certificate that contains a public encryption key, and by obtaining a service identifier that corresponds to the user request [paragraphs 0056-0057 and figures 1-2];

an authorization service configured to receive the security certificate and the service identifier from the client application, and being further configured to selectively generate a corresponding session ticket that is encrypted with the public key, the client application being further configured to receive and decrypt the corresponding session ticket with a private key that corresponds to the public key [paragraphs 0085, 0088 and figures 1-2]; and

a service provider configured to receive a service command with the corresponding session ticket after it has been decrypted, and being further configured to validate information contained in the corresponding session ticket and selectively execute the service command [paragraphs 0062, 0093-0096 and figures 1-2].

7. As per claim 21, Jancula teaches a method for enabling secure communication between a service provider and a plurality of socket applications installed on multiple computing devices within a local access network, wherein the service provider is configured to extend the functionality of the socket applications by providing services, the method comprising:

creating an account by registering with a centralized authentication service associated with the service provider, wherein registering includes indicating a desire to activate a service supported by the service provider [paragraphs 0056-0057 and 0070-0072]; and

activating each of the plurality of socket applications, wherein activating comprises:

generating a public key and a corresponding private key [paragraph 0056];

storing the private key [paragraph 0056];

transmitting the public key over the network, along with an indication of the account, to the centralized authentication service [paragraphs 0056-0057]; and

receiving from the authentication service a security certificate that includes the public key [paragraphs 0060 and 0088].

8. As per claim 26 Jancula teaches a computer-implemented method for enhancing the security of communication over a network between multiple peer application hosts, the method comprising:

receiving a security certificate from a first application host [paragraphs 0056-0057];

generating a session ticket [paragraphs 0085 and 0088];

encrypting the session ticket with a public key contained in the security certificate [paragraphs 0060 and 0088];

transmitting the session ticket to the first application host [paragraph 0088]; and

receiving a message from the first application host, the message being at least partially encrypted in accordance with the session key prior to its being encrypted with the public key [paragraphs 0091-0096].

9. As per claims 2-7, Jancula further teaches the method wherein: selectively transmitting a security certificate to the remote system comprises selectively transmitting a security certificate to a service provider configured to extend the functionality of a software application by remotely providing a service, and receiving from the user a request comprises receiving a request for a delivery of said service [paragraphs 0056-0057 and 0085].

10. As per claim 8, Jancula further teaches the method wherein selectively transmitting a security certificate comprises selectively transmitting a security certificate that contains an embedded indication of the identity of an entity associated with which the user is associated [paragraphs 0056-0057].

11. As per claims 9-11, Jancula further teaches the method wherein applying a collection of security privileges comprises applying a collection of security privileges wherein access rights are distributed among a plurality of user accounts each associated with a different set of authentication credentials [paragraphs 0057-0058 and 0071-0075].

12. As per claim 13, Jancula further teaches the method wherein using the session ticket comprises using the session ticket as a symmetric cryptography key for encrypting messages [paragraphs 0062 and 0093-0096].

13. As per claims 14-15, Jancula further teaches the method wherein transmitting the security certificate over the network comprises transmitting the security certificate to a service provider configured to extend the functionality of a software application by remotely providing a service [paragraphs 0056-0057].

14. As per claims 16-17, Jancula further teaches the method wherein transmitting the security certificate over the network comprises transmitting the certificate to a remote peer [paragraphs 0056-0057].

15. As per claim 22, Jancula further teaches the method further comprising activating one or more services [paragraphs 0056-0067].

16. As per claim 23, Jancula further teaches the method further comprising interacting with at least one socket application to configure a set of user access privileges [paragraphs 0056-0057].

17. As per claim 27, Jancula further teaches the method further comprising: generating a response message, encrypting the response message, and transmitting the message to the first application host [paragraphs 0056-0057 and 0088].

18. As per claims 19, 20, 24 and 25, Jancula further teaches the method wherein the authorization service is further configured to again encrypt the corresponding session ticket but this time with a first key portion of a service key pair [paragraph 0088].

19. As per claims 28 and 29, Jancula further teaches the method further comprising authenticating the certificate [paragraphs 0056-0057].

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Beemnet W. Dada whose telephone number is (571) 272-3847. The examiner can normally be reached on Monday - Friday (9:00 am - 5:30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Beemnet W Dada

September 25, 2007

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100